Vendor Instructions

Vendor Response Column:
Place a “**Yes**” if the current release of the software can fully support **ALL** the functionality described in the row, without special customization. A “Yes” can **only** be used if the delivery method is Standard (see delivery method instructions below). Otherwise, enter an "**No**"; A "No" can only be used with delivery method Future, Custom, or Not Available/Not Proposing (see delivery method instructions below).

Criticality Column:
(**M**) Indicates a requirement that is "**Mandatory**". The State considers it to be of such great importance that it must be met in order for the proposal to be accepted. If the proposer believes that there is something about their proposal that either obviates the need for this requirement or makes it of less importance this must be explained within the comments. The State retains the right to accept a proposal if the need of the requirement is reduced or eliminated by another feature of the proposal.
(P) Indicates a requirement which is "**Preferred**". This requirement is considered by the State to be of great usefullness but the lack of this feature is not considered serious enough to disqualify the proposal.
(O) Indicates a requirement which is "**Optional**". This requirement is considered by the State to be one which usefull or potentially usefull but not a central feature of the Project.

Delivery Method Column:
Complete the delivery method using a Standard, Future, Custom, or Not Available/Not Proposing (as defined below) that indicates how the requirement will be delivered.

Standard - Feature/Function is included in the proposed system and available in the current software release.
Future - Feature/Function will be available in a future release. (Provide anticipated delivery date, version, and service release in the comment area.)
Custom - Feature/Function can be provided with custom modifications. (Respondent must provide estimated hours and average billing rate or flat cost for the software modification in the comment area. These cost estimates should add up to the total cost for software modifications found in the cost summary table in Section X of the RFP).
Not Available/Not Proposing - Feature/Function has not been proposed by the Vendor. (Provide brief description of why this functionality was not proposed.)

Comments Column:
For all Delivery Method responses vendors must provide a brief explanation of how the requirement will be met. Free form text can be entered into this column.

BUSINESS REQUIEMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
PATIENT TRACKING					
B1.1	Solution must have the capability of two interdependent views; home view containing aggregated data from all facilities and viewable by all users and a facility specific view for each facility with viewing restricted by permission.	M			
B1.2	Solution must have the capability of integrating, managing, and tracking patient data from 30 to 50 different facilities.	M			
B1.3	Solution must have the capability of retaining base diagnostic information for patients.	M			
B1.4	Solution must track patients whether on a queue or if occupying an inventoried bed (without previously being on the queue).	M			
B1.5	***Solution must have the ability to capture, manage and track manually entered information from treatment site users identified in B1.7. Note: This functionality must be scalable for expansion of additional, yet to be identified, services/treatment providers (such as SUD, transitional housing, community residences, etc.). This level of expansion is for future phases and is not part of this project at this time.***	***M***			

B1.6	***Solution must have the ability to automatically connect with and capture, manage and track information from treatment site users identified in B1.7. In Phase I, the automated connections will apply to NHH Care Connect when it is operationalized in 2018. Note: In Phase II, these automated connections will be expanded to the balance of the user environment included in Phase I. In Future phases, this functionality must be scalable for expansion of additional, yet to be identified, services/treatment providers, such as SUD, transitional housing, community residences, etc. Phase II and Future phase expansions are not part of this project at this time.***	***M***			
B1.7	Solution must capture patient specific information including: name (or partial name), alias, DOB, gender(drop down list), partial SSN, legal status/type of admission and discharge (voluntary, involuntary, conditional discharge, revoked conditional discharge), present treatment site, new treatment site type needed, limited clinical characteristics and other health information (e.g. medication information), referral source, referral time, payer, guardian(s), preferred language, other accommodation needs, identify applicable patient queue or none, date of last admission to NHH, CMHC Client (y/n), IF y –which CMHC, number of previous NHH admissions, housing status, ward of state indicator (y/n). This functionality must be scalable for expansion of additional, yet to be identified, data.	M			

B1.8	***The solution must have the capability of interoperability to automatically receive information detailed in B1.7 from NHH Care Connect and from additional treatment site's EMRs as business agreements are executed. This functionality must be scalable for expansion of additional, yet to be identified, services/treatment providers (such as SUD, transitional housing, community residences, etc.). In Phase I, required interoperability applies to NHH Care Connect when it is operationalized in 2018. NOTE: In Phase II, interoperability will be expanded to the balance of the user enviornment included in Phase I. In future phases, expansion may be extended to other future user environments, such as SUD, transitional housing, community residences, etc. Interoperability for these Phase II and beyond is not required in Phase I.***	M			
B1.9	Solution must allow for patient information and bed availability updates from treatment site users and the Department administrator.	M			
B1.10	***Solution must have the ability to automatically import updated patient information and bed availability from NHH Care Connect and other treatment site systems and with EMR systems. In Phase I, the ability to automatically import will apply to NHH Care Connect when it is operationalized in 2018. Note: In Phase II, automated imports will be expanded to the balance of the user enviornment included in Phase I. In Future phases, expansion may be extended to other future user environments, such as SUD, transitional housing, community residences, etc. Automatic importing of patient information for Phase II and beyond is not required in Phase I.***	***M***			

B1.11	Solution must be able to sort/filter (ascending, descending) patient record data based on a variety of information fields, such as DOB, gender, admission and discharge type/legal status, present treatment site, new treatment site type needed, clinical characteristics, referral source, referral time.	M			
B1.12	Solution must automatically maintain prioritized patient queues based on referral time, legal status, adult/child, or by manual repriorization (manager level).	M			
B1.13	Solution must be able to accommodate patient specific brief note entry and retrieval (time stamped and contiguous). Notes fields must be text searchable for basic and advanced searches.	M			
BED TRACKING					
B2.1	Solution must record bed status as described below (B2.2 - B2.6):				
B2.2	Bed inventory status information to include: treatment site, bed specific characteristics/restrictions, automated bed availability status indicator based on patient occupying or leaving bed, manual bed availability update capability, payer restrictions	M			
B2.3	Potential availability status' to include: available, occupied, being held, out of service (with ETA), pending vacancy, pending admission, pending discharge.	M			
B2.4	Capture secondary status' to accommodate secondary status (one of those above).	M			
B2.5	Updated automatically upon patient transfer/manual change by treatment site.	M			
B2.6	Bed characteristics to include; voluntary, involuntary, psychiatric, SUD, age, gender, hospital, non hospital, community-other, private, non private, other.	M			

INTEROPERABILITY					
B3.1	***Solution must be capable of interoperability with NHH Care Connect to accommodate the automated transfer of patient information for triage and transfer purposes. The solution must also accommodate treatment site acceptance or deferral of a patient transfer. NHH Care Connect is anticipated to be operationalized in 2018; interoperability with it is a required component of Phase I. Note: In Phase II, interoperability will be expanded to the balance of the user enviornment included in Phase I. In Future phases, expansion may be extended to other future user environments, such as SUD, transitional housing, community residences, etc. Interoperability with other treatment providers' EMRs for Phase II and beyond is not required in Phase I.***	***M***			
B3.2	***Not used***	***N/A***			
DATA CAPTURE / INFORMATION TRANSFER					
B4.3	The solution's secure transmissions must be compliant with HIPAA and any other applicable federal or state regulation/law.	M			
NOTIFICATIONS					
B5.1	Solution must provide event-based notifications to alert applicable users of bed and patient status changes.	M			
B5.2	Solution should provide customized, user-specified notification settings that allows authorized users to specify the events they wish to be notified of based on specified treatment sites, patient legal status, patient gender, patient age (adult, child), patient progression status.	P			

B5.3	Solution must generate notifications to specified users when patient specific information and documentation is sent to them.	M			
B5.4	Solution should alert users via external communication methods (text, email,etc.) when user specific notifications are available for viewing.	P			
B5.5	Solution must generate notifications when no patient status change or update has occurred within a set amount of time.	M			
B5.6	Solution should generate escalated notifications, "Alerts", when patient in ED wait time exceeds a system set interval.	P			
B5.7	Solution should identify patients where ED wait times or inactivity exceeds defined thresholds.	P			
REPORTING					
B6.1	Solution must be able to export record level data on an ad hoc basis to enable the creation of customized reports.	M			
B6.2	Solution should provide data analytics and reporting capacity to support canned and ad hoc reporting.	P			
B6.3	Solution must have the ability to integrate with the Department's planned enterprise BI and analytic platforms.	M			
B6.4	Solution must be able to accommodate the import and export of data to create custom reports.	M			

B6.5	Solution must have the ability to generate canned reporting at specific intervals (i.e. daily, weekly, monthly, quarterly, yearly) by: patient status; admissions/discharges/transfers; bed inventory status; historical reporting.	M			
USER MANAGEMENT					
B7.1	Solution must support users with varying levels of privilege depending on the system’s functional capacity and user roles and responsibilities within the health care delivery system.	M			
B7.2	Solution must require two step authentication to enter system.	M			
B7.3	Solution must have the ability to create and terminate user accounts in real time or near real time based on State (DHHS) authorization.	M			
B7.4	Solution must have an easy authorization process for State (DHHS) to authorize user account creation and termination; such authorizations will be provided to the Vendor for execution.	M			
B7.5	Solution must accommodate/enable multiple user profiles and privilege setting – role based and/or configurable.	M			
B7.6	Solution must have a "View Only" user role, including at minimum: (see B7.7 - B7.14)	M			
B7.7	View: Legal Status: Voluntary, Involuntary, CD, RCD views	M			
B7.8	View: Admission and Discharge views	M			
B7.9	View: Payer specific	M			
B7.10	View: Referral source specific	M			
B7.11	View: Facility specific	M			
B7.12	View: All facilities	M			

B7.13	View: Gender	M			
B7.14	View: Adult - child	M			
B7.15	Solution must have an "Editor" user role, including 3 type options for designation: Facility specific, all facilities, or by referral source, such as Community Mental Health Center.	M			
B7.16	Solution "Editor" role must be able to: Add and remove patient to/from queue; Admit, discharge and transfer patient; Add patient information/documentation needed for queue progression status; input/change Legal status; allow Editor to update bed availability manually; automatically update bed availability based on specified Editor actions; automatically update the patient admit/discharge/transfer status based on specified Editor action to patient record.	M			
B7.17	Solution must have a "Manager: user role. The Manager role must be able to: add, change, remove users and set user privileges, or authorize these transactions through request to system administrator; and change prioritization of patients in the queue (ED Waitlist queue - involuntary admissions).	M			
B7.18	Solution must have a "Reporting" user role. The "Reporting" role must be tied to State specified user criteria such as, DHHS Analytics staff, the "Manager," "NHH QI Director." The "Reporting" role must be able to: export and import data to create custom reports; generate canned reporting at specific intervals (i.e. daily, weekly, monthly, quarterly, yearly) by patient status, admissions/discharges/transfers, bed inventory status.	M			

B7.19	Solution must have a "System Administrator" user role that permits two types of "System Administrators": (1) a System Administrator responsible for infrastructure and all core components; and (2) an Application Administrator responsible for functionality re: access, views, assigning user roles, permissions and restrictions, configure user views, etc.	M			
B7.20	Solution should be able to generate notifications to be received by specified users and user groups (role based) upon certain State specified user actions, such as the addition of a patient to the queue, the discharge of a patient, a patient's legal status being changed, etc. (Future Phases).	P			
USER FRIENDLINESS AND USABILITY					
B8.1	Solution should provide visualizations appropriate for data being displayed to provide quick, easy access to inpatient bed availability information, patient queue data, etc. (such as dashboard, charts, tables, lists, etc.). Visualizations must be customizable by user roles, ensure that bed types are easily distinguished, ensure that patient types are easily distinguished, and allow user views to be filtered and sorted by attributes such as: patient queue, referral queue, treatment facility queue, bed inventory, referral source queue.	P			
B8.2	Solution must provide/include Help Screens (indexed and searchable).	M			
B8.3	Solution must include FAQs.	M			
B8.4	Solution must include user documentation.	M			

B8.5	***Solution must include online training and eLearning that includes the elements described in B8.5.1 through B8.5.9.***	***M***			
B8.5.1	***Video Classrooms***	***M***			
B8.5.2	***Virtual classrooms***	***M***			
B8.5.3	***Interactive e-lessons***	***M***			
B8.5.4	***Instructor-led online training***	***M***			
B8.5.5	***Electronic simulations***	***M***			
B8.5.6	***Mobile learning***	***M***			
B8.5.7	***Self-paced***	***M***			
B8.5.8	***Online discussions***	***M***			
B8.5.9	***8:00 AM - 5:00 PM EST(M-F) chat and/or call-in online and elearning support***	***M***			
B8.6	Solution must allow users to sort/filter (ascending, descending) patient record data based on a variety of information fields, such as DOB, gender, admission and discharge type/legal status, present treatment site, new treatment site type needed, clinical characteristics, referral source, referral time.	M			
B8.7	Solution must be user friendly (easy to use and operate) for varied clinical and non clinical user groups (e.g. emergency department staff, hospital admission staff, designated receiving facility staff, mental health workers, clinicians, doctors, etc.).	M			

REFERRAL MANAGEMENT					
B9.1	Solution must enable treatment sites to enter/capture an acceptance or deferral of a patient transfer.	M			
B9.2	***Solution must be able to automatically move patient forward in progress of pre-determined steps of the queue process, from placement onto the queue to discharge, based on pre-determined user-completed actions.***	***M***			
B9.3	Solution must be able to automatically maintain prioritized patient queues based on referral time, legal status, or by manual re-priorization (manager level).	M			
B9.4	Solution must permit the manual change of prioritization of patients on the DRF/NHH queue, and for referrals to be redirected to an alternative treatment site, for State-specified users.	M			
B9.5	Solution must reconcile bed usage with patients: solution will automatically update bed availability upon the admission/discharge of a patient to the bed, regardless of whether the patient is/was on the queue for NHH.	M			
B9.6	Solution must release patient specific information for viewing by specified treatment sites and providers based on roles. Viewable patient information, such as: name, DOB, gender, partial SSN, type of admission and discharge (voluntary, involuntary, conditional discharge, revoked conditional discharge), will be customized per State specified user roles/privileges. Solution must release/transfer, on a similar basis, information from/thru/to treatment site EMRs, networked tools, shared care plans as State specified and interoperability, business agreements, are developed/achieved.	M			
B9.7	Solution must track input by user ID.	M			

B9.8	Solution must track final patient disposition, to include State specified information fields, such as authorized by, date and time.	M			
B9.9	Solution must maintain a full audit trail on a patient specific basis from beginning to end of a patient being added into the system and later discharged. With electronic signature capability.	M			
SCALABILITY / PHASING					
B10.1	Solution must be of modular design.	M			
B10.2	***Solution must be configurable to support a phased-in approach that can flexibly accommodate the variety of different users, and varying functional capacities of treatment providers' own EMRs. In Phase I, this must include the ability for treatment sites to manually enter patient information into the Solution and for the Solution to populate corresponding information fields to create the patient referrals that will be managed by the Solution. Also in Phase I, the Solution must be able to accommodate NHH's single-entry of additional patient information (post initial referral) into NHH Care Connect (when it is operationalized in 2018) and that information is automatically captured by the Solution. Note: In Phase II, this must include the ability for single-entry of initial patient information (completed at the treatment site by entering patient information into the site's EMR and automatically capturing such information into the Solution to populate corresponding information fields necessary to create the patient referral that will be managed within the Solution). In Future phases, the Solution must be able to accommodate additional treatment site's EMRs as business agreements are reached for this purpose. Phase II and Future phase capabilities are not part of the requirements at this time.***	***M***			

B10.3	Solution must be flexible and able to accommodate a variety of different user groups, with additional groups added in subsequent phases.	M			
B10.5	Solution must fulfill the baseline requirement in HB517 – an integrated data management system that provides real-time or near real-time information about the availability of involuntary and voluntary inpatient psychiatric beds in the state of New Hampshire.	M			
B10.6	Solution must use patient specific information to support and streamline patient triage and transfer from one treatment site to another.	M			
B10.7	Solution must use patient specific information to support and streamline discharge out of an inpatient psychiatric bed.	M			
B10.8	Solution must provide data analytic capacity to support tracking of patient and bed statistics and reporting of record level data.	M			
VENDOR RESPONSIBILITIES					
B11.1	***Vendor must be responsible for conducting a one-month project readiness assesment for Phase I within the first thirty (30) days of contract effective date, a Phase II project readiness assessment within the first six months (180 days) of contract effective date, and final report within 30-days after contract termination.***	***M***			

B11.2	***Vendor must be responsible for conducting and working with the Department's project team to identify and separate system requirements into four categories within the project's two phases (Phase I and Phase II):*** ***• Bed tracking (all treatment sites), and data sharing with NHH Care Connect (Phase I)*** ***• Patient waitlist/queue management (all treatment sites) (Phase I)*** ***• Facilitate the referral, assessment and transfer of patients in need of acute psychiatric care, electronically categorize, capture and share the patient's mental health and medical need, mental health facility type, and appropriate bed type and merge with the bed-tracking system. Note: In Phase I, treatment sites will manually input information into the Solution for this purpose; also in Phase I, interoperability with NHH Care Connect (to be operationalized in 2018) will support this with additional automation. In Phase II, interoperability with the balance of the treatment sites will support this additional automation. In Future phases, this may be expanded to other treatment and provider communities. Phase II and Future phases are not required at this time.*** ***• IDMS interoperability with treatment sites' Electronic Health Records (EHRs)/Electronic Medical Records (EMRs) to automatically connect and update patient status. Note: the phased in approach described in the previous bullet applies to interoperability as well.***	***M***			
B11.3	***Vendor must be responsible for identifing new requirements, reviewing, and confirming requirements and/or additions at the beginning of each phase within DDI.***	***M***			
B11.4	***Vendor must be responsible for Phase I Solution design and providing the Deparment with a Phase I solution design document inclusive, at minimum, of diagram and plan.***	***M***			

B11.5	Vendor must be responsible for Phase I Solution development and providing the Deparment with a development design diagram and plan.	M			
B11.6	Vendor must be responsible for implementation services and providing the Deparment with a Phase I implementation design diagram and plan.	M			
B11.7	Vendor must be responsible for project management.	M			
B11.8	Vendor must develop a training plan, that addresses all of the components in B.8.5 above, and applicable training documentation.	M			
B11.9	Vendor must provide online training as described in B.8.5 above.	M			
B11.10	Vendor must provide on-site training as described in B.8.5 above.	M			
B11.11	Vendor must be responsible for report development (i.e. standard and ad hoc).	M			
B11.12	Vendor must be responsible for developing an operations manual that details installation as well as maintenance.	M			
B11.13	Vendor must be responsible for maintenance and support services as further described herein.	M			
B11.14	Vendor must be responsible to implement Vendor modifications.	M			
B11.15	Vendor must be responsible for testing services.	M			

APPLICATION REQUIREMENTS					
State Requirements			**Vendor**		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
GENERAL SPECIFICATIONS					
A1.1	Ability to access data using open standards access protocol (please specify supported versions in the comments field).	M			
A1.2	Data is available in commonly used format over which no entity has exclusive control, with the exception of National or International standards. Data is not subject to any copyright, patent, trademark or orhter trade secret regulation.	M			
A1.3	Web-based compatible and in conformance with the following W3C standards: HTML5, CSS 2.1, XML 1.1, HL7-2.X, HTTPS V2.X	M			
APPLICATION SECURITY					
A2.1	Verify the ***identity or authenticate*** all of the system client applications before allowing use of the system to prevent access to inappropriate or confidential data or services.	M			
A2.2	Verify the ***identity*** ***and*** ***authenticate*** all of the system's human users before allowing them to use its capabilities to prevent access to inappropriate or confidential data or services. .	M			
A2.3	Enforce unique user names.	M			
A2.4	Enforce complex passwords for Administrator Accounts in accordance with DoIT's statewide *User Account and Password Policy*	M			

Table C-2 Addendum 1:
General Requirements Vendor Response Checklist

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
A2.5	Enforce the use of complex passwords for general users using capital letters, numbers and special characters in accordance with DoIT's statewide User Account and Password Policy.	M			
A2.6	Encrypt passwords in transmission and at rest within the database.	M			
A2.7	Establish ability to expire passwords after a definite period of time in accordance with DoIT’s statewide User Account and Password Policy	M			
A2.8	Provide the ability to limit the number of people that can grant or change authorizations	M			
A2.9	Establish ability to enforce session timeouts during periods of inactivity.	M			
A2.10	***The application must not store authentication credentials or sensitive data in its code.***	***M***			
A2.11	Log all attempted accesses that fail identification, authentication and authorization requirements.	M			
A2.12	***The application must log all activities to a central server to prevent parties to application transactions from denying that they have taken place.***	***M***			
A2.13	All logs must be kept for two years	M			
A2.14	The application must allow a human user to explicitly terminate a session. No remnants of the prior session should then remain.	M			

Table C-2 Addendum 1:
General Requirements Vendor Response Checklist

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
A2.15	Do not use Software and System Services for anything other than they are designed for.	M			
A2.16	***The application Data must be protected from unauthorized use when at rest***	***M***			
A2.17	***The application must keep any sensitive Data or communications private from unauthorized individuals and programs.***	***M***			
A2.18	***Subsequent application enhancements or upgrades must not remove or degrade security requirements***	***M***			
A2.19	Utilize change management documentation and procedures	M			
A2.20	***Web Services: The service provider must use Web services exclusively to interface with the State's data in near real time when possible.***	***M***			

TESTING					
State Requirements			**Vendor**		
Req #	**Requirement Description**	**Criticality**	**Vendor Response**	**Delivery Method**	**Comments**
APPLICATION SECURITY TESTING					
T1.1	***All components of the Software must be reviewed and tested to ensure they protect the State’s web site and its related Data assets.***	***M***			
T1.2	***The Vendor must be responsible for providing documentation of security testing, as appropriate. Tests must focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide the necessary confidentiality, integrity and availability.***	***M***			
T1.3	Provide evidence that supports the fact that Identification and Authentication testing has been recently accomplished; supports obtaining information about those parties attempting to log onto a system or application for security purposes and the validation of users	M			
T1.4	Test for Access Control; supports the management of permissions for logging onto a computer or network	M			
T1.5	Test for encryption; supports the encoding of data for security purposes, and for the ability to access the data in a decrypted format from required tools.	M			
T1.6	Test the Intrusion Detection; supports the detection of illegal entrance into a computer system	M			

T1.7	Test the Verification feature; supports the confirmation of authority to enter a computer system, application or network	M			
T1.8	Test the User Management feature; supports the administration of computer, application and network accounts within an organization.	M			
T1.9	Test Role/Privilege Management; supports the granting of abilities to users or groups of users of a computer, application or network	M			
T1.10	Test Audit Trail Capture and Analysis; supports the identification and monitoring of activities within an application or system	M			
T1.11	Test Input Validation; ensures the application is protected from buffer overflow, cross-site scripting, SQL injection, and unauthorized access of files and/or directories on the server.	M			
T.1.12	***For web applications, ensure the application has been tested and hardened to prevent critical application security flaws. (At minimum, the application must be tested against all flaws outlined in the Open Web Application Security Project (OWASP) Top Ten (http://www.owasp.org/index.php/OWASP_Top_Ten_Project))***	***M***			
T1.13	Provide the State with validation of 3rd party security reviews performed on the application and system environment. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review (please specify proposed methodology in the comments field).	M			

T1.14	***Prior to the System being moved into production, the Vendor must provide results of all security testing to the Department of Information Technology for review and acceptance.***	***M***			
T1.15	***Vendor must provide documented procedure for migrating application modifications from the User Acceptance Test Environment to the Production Environment.***	***M***			
T1.16	***As part of the risk assessment process the Vendor must conduct a penetration test to identify vulnerabilities in any web applications, internal devices, Internet-facing IP addresses and applications and link them to identifiable threats. Costs for penetration tests must be the Vendor's responsibility.***	***M***			
T1.17	***As part of the risk mitigation plan the Vendor must conduct a penetration test to ensure that controls work as designed. Costs for penetration tests must be the Vendor's responsibility.***	***M***			
T1.18	***The Vendor must issue a final report with respect to Pen testing that addresses any deficiencies found during Pen testing.***	***M***			
STANDARD TESTING					
T2.1	The Vendor must test the software and the system using an industry standard and State approved testing methodology as more fully described in in Appendix G, Security, Testing and Certificates, Section 2 - Testing Requirements.	M			
T2.2	The Vendor must perform application stress testing and tuning as more fully described in Appendix G, Security, Testing and Certiicates, Section 2 - Testing Requirements.	M			
T2.3	The Vendor must provide documented procedure for how to sync Production with a specific testing environment.	M			
T2.4	The vendor must define and test disaster recovery procedures.	M			
T2.5	The vendor must define and test redundancy procedures.	M			

HOSTING-CLOUD REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
OPERATIONS					
H1.1	***Vendor must provide an ANSI/TIA-942 Tier 3 Data Center or equivalent. A tier 3 data center requires 1) Multiple independent distribution paths serving the IT equipment, 2) All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture and 3)Concurrently maintainable site infrastructure with expected availability of 99.982%***	***M***			
H1.2	***Vendor must maintain a secure hosting environment providing all necessary hardware, software, and Internet bandwidth to manage the application and support users with permission based logins.***	***M***			
H1.3	***The Data Center must be physically secured – restricted access to the site to personnel with controls such as biometric, badge, and others security solutions. Policies for granting access must be in place and followed. Access must only be granted to those with a need to perform tasks in the Data Center.***	***M***			
H1.4	***Vendor must install and update all server patches, updates, and other utilities within 60 days of release from the manufacturer.***	***M***			
H1.5	***Vendor must monitor System, security, and application logs.***	***M***			
H1.6	***Vendor must manage the sharing of data resources.***	***M***			
H1.7	***Vendor must manage daily backups, off-site data storage, and restore operations.***	***M***			

H1.8	***The Vendor must monitor physical hardware.***	***M***			
H1.9	***Remote access must be customized to the State's business application. In instances where the State requires access to the application or server resources not in the DMZ, the Vendor must provide remote desktop connection to the server through secure protocols such as a Virtual Private Network (VPN).***	***M***			
H1.10	***The Vendor must report any breach in security in conformance with State of NH RSA 359-C:20. Any person engaged in trade or commerce that is subject to RSA 358-A:3, I must also notify the regulator which has primary regulatory authority over such trade or commerce. All other persons must notify the New Hampshire attorney general's office.***	***M***			
DISASTER RECOVERY					
H2.1	***Vendor must have documented disaster recovery plans that address the recovery of lost State data as well as their own. Systems must be architected to meet the defined recovery needs.***	***M***			
H2.2	***The disaster recovery plan must identify appropriate methods for procuring additional hardware in the event of a component failure. In most instances, systems must offer a level of redundancy so the loss of a drive or power supply will not be sufficient to terminate services however, these failed components will have to be replaced.***	***M***			
H2.3	***Vendor must adhere to a defined and documented back-up schedule and procedure.***	***M***			
H2.4	Back-up copies of data are made for the purpose of facilitating a restore of the data in the event of data loss or System failure.	M			
H2.5	***Scheduled backups of all servers must be completed regularly. The minimum acceptable frequency is differential backup daily, and complete backup weekly.***	***M***			

H2.6	Tapes or other back-up media tapes must be securely transferred from the site to another secure location to avoid complete data loss with the loss of a facility.	M			
H2.7	***Data recovery – In the event that recovery back to the last backup is not sufficient to recover State Data, the Vendor must employ the use of database logs in addition to backup media in the restoration of the database(s) to afford a much closer to real-time recovery. To do this, logs must be moved off the volume containing the database with a frequency to match the business needs.***	***M***			
HOSTING SECURITY					
H3.1	***The Vendor must employ a FedRAMP compliant soution.***	***M***			
H3.2	***The Vendor must employ security measures ensure that the State's application and data is protected.***	***M***			
H3.3	If State data is hosted on multiple servers, data exchanges between and among servers must be encrypted.	M			
H3.4	***All servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, must have aggressive intrusion-detection and firewall protection.***	***M***			
H3.5	***All components of the infrastructure must be reviewed and tested to ensure they protect the State's hardware, software, and its related data assets. Tests must focus on the technical, administrative and physical security controls that have been designed into the System architecture in order to provide confidentiality, integrity and availability.***	***M***			

H3.6	***The Vendor must ensure its complete cooperation with the State’s Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure.***	***M***			
H3.7	***The Vendor must authorize the State to perform scheduled and random security audits, including vulnerability assessments, of the Vendor’ hosting infrastructure and/or the application upon request.***	***M***			
H3.8	***All servers and devices must have event logging enabled. Logs must be protected with access limited to only authorized administrators. Logs shall include System, Application, Web and Database logs.***	***M***			
H3.9	***Operating Systems (OS) and Databases (DB) must be built and hardened in accordance with guidelines set forth by CIS, NIST or NSA.***	***M***			
H3.10	***The Vendor must notify the State’s Project Manager of any security breaches within two (2) hours of the time that the Vendor learns of their occurrence.***	***M***			
H3.11	***The Vendor must be solely liable for costs associated with any breach of State data housed at their location(s) including but not limited to notification and any damages assessed by the courts.***	***M***			
H3.12	***An application security review and penetration tests required when there are any substantial change in application code by the Vendor. At the least, the Vendor is required to submit attestation that the penetration testing and review has been completed.***	***M***			

SERVICE LEVEL AGREEMENT					
H4.1	The Vendor's System support and maintenance must commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.	M			
H4.2	The Vendor must maintain the hardware and Software in accordance with the specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
H4.3	The Vendor must repair or replace the hardware or software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
H4.4	All hardware and software components of the Vendor hosting infrastructure must be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc, must be applied within sixty (60) days of release by their respective manufacturers.	M			
H4.5	The State must have unlimited access, via phone or Email, to the Vendor technical support staff 24/7/365.	M			
H4.6	The Vendor must conform to the specific deficiency class as described: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.	M			

H4.7	As part of the maintenance agreement, ongoing support issues must be responded to according to the following: a. Class A Deficiencies - The Vendor must have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor must provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State must notify the Vendor of such Deficiencies during regular business hours and the Vendor must respond back within four (4) hours of notification of planned corrective action; The Vendor must repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract;	M			
H4.8	The hosting server for the State must be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M			
H4.9	A regularly scheduled maintenance window must be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades must be applied.	M			
H4.10	If The Vendor is unable to meet the uptime requirement, the Vendor shall credit State's account in an amount based upon the following formula: (Total Contract Item Price/365) x Number of Days Contract Item Not Provided. The State must request this credit in writing.	M			
H4.11	The Vendor must use a change management policy for notification and tracking of change requests as well as critical outages.	M			
H4.12	A critical outage must be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.	M			
H4.13	The Vendor must maintain a record of the activities related to repair or maintenance activities performed for the State and must report quarterly on the following: Server up-time; All change requests implemented, including operating system patches; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
H4.14	The Vendor must give thirty-business days prior notification to the State Project Manager of all scheduled changes/updates and provide the State with training due to the upgrades and changes.	M			

SUPPORT & MAINTENANCE REQUIREMENTS					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
SUPPORT & MAINTENANCE REQUIREMENTS					
S1.1	***The Vendor's System support and maintenance must commence upon the Effective Date and extend through the end of the Contract term, and any extensions thereof.***	***M***			
S1.2	Maintain the hardware and Software in accordance with the Specifications, terms, and requirements of the Contract, including providing, upgrades and fixes as required.	M			
S1.3	Repair Software, or any portion thereof, so that the System operates in accordance with the Specifications, terms, and requirements of the Contract.	M			
S1.4	***The State must have unlimited access, via phone or Email, to the Vendor technical support staff 24/7/365;***	***M***			
S1.5	***The Vendor response time for support must conform to the specific deficiency class as described below or as agreed to by the parties: o Class A Deficiency - Software - Critical, does not allow System to operate, no work around, demands immediate action; Written Documentation - missing significant portions of information or unintelligible to State; Non Software - Services were inadequate and require re-performance of the Service. o Class B Deficiency - Software - important, does not stop operation and/or there is a work around and user can perform tasks; Written Documentation - portions of information are missing but not enough to make the document unintelligible; Non Software - Services were deficient, require reworking, but do not require re-performance of the Service. o Class C Deficiency - Software - minimal, cosmetic in nature, minimal effect on System, low priority and/or user can use System; Written Documentation - minimal changes required and of minor editing nature; Non Software - Services require only minor reworking and do not require re-performance of the Service.***	***M***			

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S1.6	***The Vendor must make available to the State the latest program updates, general maintenance releases, selected functionality releases, patches, and Documentation that are generally offered to its customers, at no additional cost.***	***M***			
S1.9	For all maintenance Services calls, The Vendor should ensure the following information will be collected and maintained: 1) nature of the Deficiency; 2) current status of the Deficiency; 3) action plans, dates, and times; 4) expected and actual completion time; 5) Deficiency resolution information, 6) Resolved by, 7) Identifying number i.e. work order number, 8) Issue identified by;	P			
S1.10	The Vendor must work with the State to identify and troubleshoot potentially large-scale System failures or Deficiencies by collecting the following information: 1) mean time between reported Deficiencies with the Software; 2) diagnosis of the root cause of the problem; and 3) identification of repeat calls or repeat Software problems.	M			
S1.11	As part of the Software maintenance agreement, ongoing software maintenance and support issues, must be responded to according to the following or as asgreed to by the parties: a. Class A Deficiencies - The Vendor must have available to the State on-call telephone assistance, with issue tracking available to the State, eight (8) hours per day and five (5) days a week with an email / telephone response within two (2) hours of request; or the Vendor shall provide support on-site or with remote diagnostic Services, within four (4) business hours of a request; b. Class B & C Deficiencies –The State must notify the Vendor of such Deficiencies during regular business hours and the Vendor shall respond back within four (4) hours of notification of planned corrective action; The Vendor must repair or replace Software, and provide maintenance of the Software in accordance with the Specifications, Terms and Requirements of the Contract; or as agreed between the parties	M			

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S1.12	The Vendor must use a change management policy for notification and tracking of change requests as well as critical outages.	M			
S1.13	***A critical outage must be designated when a business function cannot be met by a nonperforming application and there is no work around to the problem.***	***M***			
S1.14	The Vendor must maintain a record of the activities related to repair or maintenance activities performed for the State and must report quarterly on the following: All change requests implemented; All critical outages reported including actual issue and resolution; Number of deficiencies reported by class with initial response time as well as time to close.	M			
S1.15	The hosting server for the State must be available twenty-four (24) hours a day, 7 days a week except for during scheduled maintenance.	M			
S1.16	The Vendor will guide the State with possible solutions to resolve issues to maintain a fully functioning, hosted System.	M			
S1.17	A regularly scheduled maintenance window must be identified (such as weekly, monthly, or quarterly) at which time all relevant server patches and application upgrades shall be applied.	M			
S1.18	The Vendor must give two-business days prior notification to the State Project Manager of all changes/updates and provide the State with training due to the upgrades and changes.	M			
S1.19	All hardware and software components of the Vendor hosting infrastructure must be fully supported by their respective manufacturers at all times. All critical patches for operating systems, databases, web services, etc, must be applied within thirty (30) days of release by their respective manufacturers.	M			
S1.20	The Vendor must provide the State with a personal secure FTP site to be used the State for uploading and downloading files if applicable.	M			
S1.21	***As part of the Software Maintenance Agreement, for continual system improvement, the Vendor must provide annual penetration (pen) testing at no additional cost.***	***M***			

Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
S1.22	***As part of the Software Maintenance Agreement, for continual system improvement, the Vendor must maintain software components at curent released level and never to exceed one revision lower, at no additional cost.***	***M***			

PROJECT MANAGEMENT					
State Requirements			Vendor		
Req #	Requirement Description	Criticality	Vendor Response	Delivery Method	Comments
PROJECT MANAGEMENT					
P1.1	Vendor must participate in an on-site initial kick-off meeting to initiate the Project.	M			
P1.2	Vendor must participate on-site for all project related meetings, unless otherwise specified by the Department.	M			
P1.3	Vendor must provide Project Staff as specified in the RFP.	M			
P1.4	Vendor must submit a finalized Work Plan within ten (10) days after Contract award and approval by Governor and Council. The Work Plan must include, without limitation, a detailed description of the Schedule, tasks, Deliverables, critical events, task dependencies, and payment Schedule. The plan must be updated no less than every two weeks.	M			
P1.5	Vendor must provide detailed bi-weekly status reports on the progress of the Project, which will include expenses incurred year to date.	M			
P1.6	All user, technical, and System Documentation as well as Project Schedules, plans, status reports, and correspondence must be maintained as project documentation. (Define how- WORD format- on-Line, in a common library or on paper)	M			
P1.7	Vendor must provide a project risk and issue management plan	M			